Charles W. Robinson
Public Sector Leader, Quantum Computing
IBM

House Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
House Committee on Homeland Security
Securing the Future: Harnessing the Potential of Emerging Technologies While Mitigating Security Risks

June 22, 2022

Introduction

Chairwoman Clarke, Ranking Member Garbarino, and distinguished members of the subcommittee, I am honored to appear before you today to discuss how to harness the benefits of emerging technologies, particularly quantum, while mitigating the potential national security consequences before this important subcommittee.

My name is Charles Robinson, and I am IBM's Quantum Computing Public Sector Leader. In addition to serving in corporate America, I've had the great privilege and honor to serve in the United States Navy. Today, I have the pleasure of supporting the preparation of the National Security Community for the Quantum Computer Age.

Leveraging the power of emerging technology while bolstering our national security is an increasingly complex mission which demands dynamic solutions and collective actions by industry and government. While these technologies promise to produce immense value to our society, new threats related to these disruptive emerging technologies create a multitude of challenges to securing and protecting people, the nation, and information. To mitigate these threats, we must understand these technologies and take actions today to prepare us for tomorrow.

My testimony will explain how we can do this effectively through collaboration. First, it is important to level set and provide a brief explanation of quantum, its importance to society, and its relationship to national security. Just as important is understanding what industry, academia, and government can do today to promote quantum resistant encryption and strengthen national security tomorrow.

What is quantum – its importance and relationship to national security

Quantum computing is not simply a faster way of doing what today's computers do – it is a fundamentally different approach that promises to solve problems that classical computing cannot realistically solve.

Quantum computers are not simply more powerful supercomputers. Instead of computing with the traditional bit of a 1 or 0, quantum computers use quantum bits, or qubits (CUE-bits), that can run multidimensional quantum algorithms.

Think of it this way, a classical supercomputer solves a problem sequentially. Supercomputers leverage their many processors to explore every possible path to a solution before arriving at an answer. But as the problem and data grow more complex, there simply isn't enough computing power to solve problems that grow exponentially. For example, there are 40 thousand different ways to seat 8 people around a table. If you add one person, it becomes 362 thousand. Make it 10 people and the number of combinations is more than 3.5 million. Eleven people, almost 40 million. No existing computer has the working memory to handle all the possible combinations as problem sizes grow exponentially large. By contrast, a quantum computer can double the size of the problem space it can analyze by adding only one qubit.

A. Quantum and its Value

Quantum algorithms take a new approach to these sorts of complex problems – creating multidimensional spaces where the patterns linking individual data points emerge. For example, in the case of the protein folding problem, where a chain of 100 amino acids could theoretically fold into trillions of ways, the optimal pattern is the combination of folds requiring the least energy to be viable. Compared to today's supercomputers, a quantum computer could find that combination of folds faster enabling the prediction of protein structures to address diverse use cases from drug discovery to agriculture.

Through these vastly improved chemical simulations in drug discovery and development, quantum computing can help expedite the response to future pandemics, ongoing health crises, and the proliferation of debilitating diseases affecting millions worldwide. Today, between one and two percent of the global energy output goes into making ammonia-based fertilizer through the nitrogen fixation process. If quantum simulations can find a way to use even a fraction less energy in that process, it would have a significant impact. Quantum computing holds the promise to help humanity confront these and many other important challenges, from solving long-standing questions in science to overcoming obstacles in improving industrial efficiency. Working in conjunction with classical computers and cloud-based architectures, quantum computers could even find answers to problems we haven't yet dreamed of. The opportunities for society and the economy are potentially limitless.

The future of this technology is truly exciting – it's likely that by the middle of this decade, we'll see applications of quantum computing that will solve practical problems faster, cheaper, or with more accuracy than classical computers. We call this the Quantum Advantage. It is essential the U.S. rapidly strives to leverage this advantage. As early adopters, we will have the opportunity to lock in economic and strategic advantages that will be enormously difficult to challenge.

B. Quantum and National Security

As we transition into an era in which quantum computers become more ubiquitous, the digital platforms that underpin our government, commerce, education, and healthcare systems may become increasingly vulnerable. This vulnerability to the technological fabric we depend on every day puts our national security at risk. However, we can protect against this via concurrent development and adoption of quantum-safe cryptography.

Simply put, quantum computers pose a challenge for a key part of our digital life: encryption.

When you send an email, make an online purchase, or make a withdrawal from an ATM, cryptography helps keep your data private and authenticate your identity.

Today's cryptographic algorithms derive their strength from the difficulty of solving certain math problems using classical computers or searching for the right secret key or message.

Quantum computers, however, work in a fundamentally different way. Solving a problem that might take millions of years on a classical computer may take hours or minutes on a sufficiently large quantum computer, which will have a significant impact on the encryption, hashing, and public key algorithms we use today. This is where quantum-safe cryptography comes in.

Let me be clear: while we do not currently have quantum computers that can break today's widely used cryptography, we expect significant advancements in the coming years, and although we already know how to perform encryption that will be resistant to a quantum computer's attack, these foundational quantum-safe algorithms should only be considered the start.

Many industry security standards and protocols need to be updated with these new algorithms, and advances in quantum computing will need to coincide with advances in quantum-safe cryptography to ensure data and systems are secured now from these future threats.

So how do we get there?

Preparing for Tomorrow by Future-Proofing in the Present - Industry & Government Collaboration & Policy

Policymakers and industry need to look to mitigate against these risks by future-proofing in the present.

A. Industry Collaborations

IBM is taking action now. Our researchers are developing practical cryptographic solutions that are resistant to the threats posed by quantum computers. We have identified a number of

cryptographic schemes that are believed to be quantum-safe. These include lattice-based cryptography, hash trees, multivariate equations, and super-singular isogeny elliptic curves.

The key advantage of such quantum-safe schemes is the absence of an exploitable structure in the mathematical problem an attacker needs to solve in order to break the encryption. Certain quantum-safe schemes (e.g., supersingular isogeny) will protect us against particularly patient attackers who store their victims' encrypted messages today only to decrypt them with new and more powerful methods in the future. Other encryption schemes (e.g., lattice cryptography) can enable game-changing technologies like Fully Homomorphic Encryption (FHE), in which data can be directly computed in encrypted form, stymieing a common strategy of attackers to loiter in a victim's computer system until sensitive data is decrypted to be used. Existing encryption today can only protect data when stored and in transit. This new technique closes this vulnerability by keeping data encrypted while it is in use.

Moreover, development of quantum-safe systems, which are systems that leverage the use of both quantum-safe cryptography as well as other security mechanisms like secure boot (meaning that bad actors cannot inject malware into the boot process to take over the system during startup) is crucial to ensure the security of systems now and in the future. IBM has invested in these technologies with its development of the industry's first quantum-safe system, the IBM z16.

To advance these and other innovative new methods for securing data in an age of quantum computing, we are collaborating with academic institutions – such as the State University of New York at Stony Brook and the University of Notre Dame – to advance the science behind these techniques.

B. U.S. Government – the critical role of government

IBM joins others in industry to work with our government to strengthen our future national security. Key among these activities is the work of the National Institute of Standards and Technology (NIST), which initiated a Post-Quantum Cryptography Standardization Program to identify new algorithms that can resist threats posed by quantum computers.

After three rounds of evaluation, NIST identified seven finalists. It plans to select a small number of new quantum-safe algorithms this year and implement new quantum-safe standards by 2024. As part of this program, IBM Researchers have been involved in the development of three quantum-safe cryptographic algorithms based on lattice cryptography that are in the final round of consideration: CRYSTALS-Kyber, CRYSTALS-Dilithium and Falcon.

More must be done to supplement private industry's engagement in standards development and to accelerate investments in, and to promote the adoption of, quantum-safe cryptographic schemes that can safeguard data now and long into the future.

C. Policy Recommendations

As I just shared, companies and governments are preparing for a quantum computing future and positioning themselves to capture the many benefits of this technology. Yet more can and should be done. Collaboration among all stakeholders is key to making progress. Governments, researchers, academics, and industry must work together on policies to accelerate the adoption of new educational curricula, fund R&D, future proof encryption, create new talent pipelines, and more.

As the U.S. government considers how best to protect national security and prepare for our quantum future, IBM recommends Congress consider policies that would:

Accelerate quantum science and the use of quantum computing – Significant investments to keep America at the forefront of the quantum computing race. Congress should support funding for fundamental research in quantum theory, hardware, and software; the rapid deployment of advanced, reliable quantum systems; and "proof of concept" programs for the U.S government to purchase commercial-grade quantum technologies. Specifically, we urge passage of:

- The Quantum User Expansion for Science and Technology program (QUEST) Act with $30M of funding to increase access to U.S. quantum computing hardware and quantum computing clouds for research, thereby accelerating U.S. economic development and national security; and
- a final Bipartisan Innovation Act (BIA), including increased funding for the Department of Energy's work as well as Quantum Network Infrastructure and Workforce Development support, which will bolster research in quantum networking and communications.

Expand and diversify the ecosystem – Support and fund initiatives that help build a robust enabling technology ecosystem of industry and academia players, as well as a supply chain for the quantum industry. This includes promoting education and training to expand the necessary workforce to make the industry sustainable as was called for in the Presidential Directives to Advance Quantum Technologies. Congress should also help to advance and expand existing initiatives such as:

- Reauthorization of the National Quantum Initiative Act for another five years to ensure continued support of Multidisciplinary Centers for Quantum Research and Education and National Quantum Information Science Research Centers to accelerate scientific breakthroughs in quantum science and technology;
- Quantum Economic Development Consortium (QED-C) to build up quantum industry supply chains;
- NSF's Q2Work and similar post-secondary studies and high-school education; and
- programs promoting greater diversity among this emerging workforce (e.g., IBM's HBCU Quantum Center) to ensure we have a quantum era ready workforce; and

- opensource research and development projects that enable the creation of platforms such as Qiskit, an open-source software development kit, that provides tools to create and manipulate quantum programs and run them on prototype quantum devices.

Future proof encryption now – Accelerate efforts around new quantum-safe cryptographic methods and prioritize workstreams to establish a quantum-safe infrastructure that has cryptographic agility (a flexible approach that enables future updates without major changes to the existing infrastructure). History has shown broad adoption of new cryptography can take more than a decade, thus we must act now. This acceleration was also called for in the Presidential Directives, which IBM strongly supports. On this, we encourage Congress to:

- Obtain from NIST an update on its Post-Quantum Cryptography Standardization Program and its National Cybersecurity Center of Excellence (NCCoE) plan for the replacement of hardware, software, and services that use public-key algorithms so that information is protected from future attacks;
- accelerate the legislative process to pass the Quantum Computing Cybersecurity Preparedness Act, which prioritizes the migration to post-quantum cryptography; and
- encourage NIST and other relevant agencies to prioritize the engagement with standards development organizations that are updating system-relevant industry standards, including those for critical infrastructure and financial industry, such as: ISO 27001, COBIT, NIST SP 800-53, ANSI/ISA-62443, and standards developed by the Council on Cybersecurity Critical Security Controls.

Encourage responsible collaboration with international partners – Leverage existing global engagements and create new ones as needed to review and ensure military and commercial trade agreements are addressing post quantum cryptography. Further, Congress should:

- Encourage the Department of State, through its new Bureau of Cyberspace and Digital Policy, and the Department of Defense to find new ways to work collaboratively with our allies and partners to promote quantum innovation and accelerate the adoption of quantum-safe encryption; and,
- support the tailoring of export controls to keep sensitive technologies out of the hands of nefarious actors given the sensitive nature of quantum R&D and that its technological components present possible dual-use concerns.

Conclusion

We don't know exactly when a large-scale quantum computer capable of breaking public key cryptographic algorithms will be available, but some experts predict this could be possible by the end of the decade. While we have some time to implement policies that counter developing threats and develop quantum-safe solutions, these years go fast, so we must act now to ensure the U.S. reaps the benefits of quantum computing while protecting our national security.

Moving to new cryptography is complex and will require significant time and investment. As a starting point, we urge Congress to meet this challenge by passing a final BIA without delay and

accelerating the legislative process on QUEST and the Quantum Computing Cybersecurity Preparedness Act.

If we continuing to work collaboratively and take the actions I just described, we will be better prepared, and our nation will be more secure for it.

Thank you.